SAND2014-3227C

Risk Analysis, Non-proliferation, and Nuclear Terrorism

Jason C. Reinhardt
Stanford University
Sandia National Laboratories

Presented to the
Moscow Engineering and Physics Institute
24 April, 2014

Sandia National Laboratories is a multi-program laboratory operated and managed by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Questions to Address

- Why is risk analysis necessary?
- What has been done?
- Why hasn't it been more successful?
- How can we move forward?

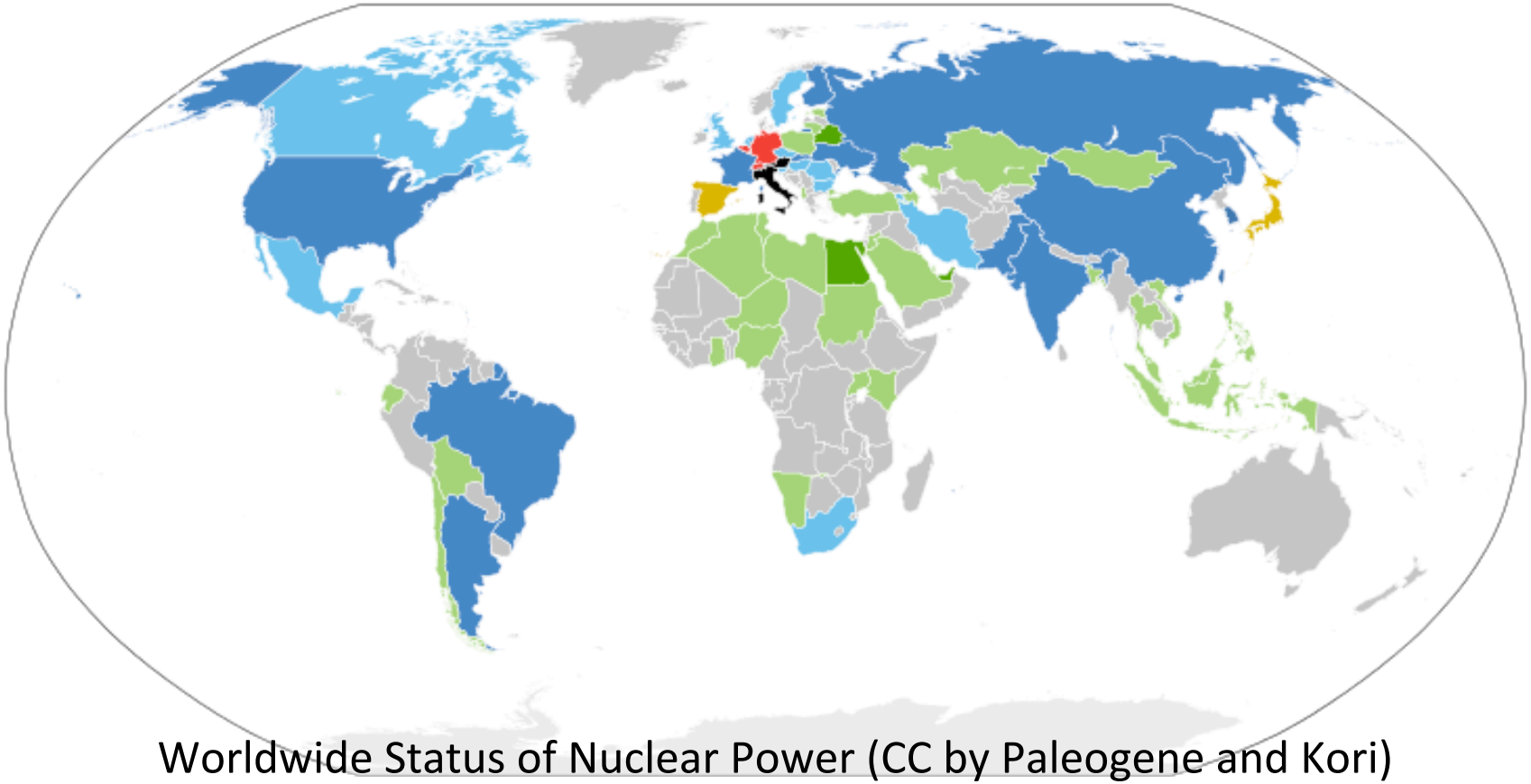
Focus will be on countering nuclear terrorism, but findings and assessment are applicable to nuclear proliferation as well.

What is the goal in combatting nuclear terrorism?

Adversaries choose not to pursue nuclear or radiological threats as a means of aggression, because they believe:

1. Use of such devices is abhorrent to the influential
2. Plans to do so will be discovered by defenders
3. Materials are too difficult to obtain
4. Materials are too difficult to weaponize
5. Materials and devices will be detected if moved
6. Emplacement of materials or devices is too difficult
7. Detonation of devices is too difficult
8. Consequences of a detonation are unsatisfactory
9. Attribution of an attack is assured
10. Retribution is unacceptable

It is a persistent threat that nations must work together to manage.



Worldwide Status of Nuclear Power (CC by Paleogene and Kori)

Intentional Actors

Nuclear technology more accessible

Conflicts between states, non-states

Illicit Trade and Black Markets

Factors with Limited Control

Mistakes and accidents

Failures and collapses

Time and chance

Important questions surround nuclear proliferation and terrorism defense.

- Which protective measures are worth the investment and implementation? What mix?
  - People and skills
  - Physical security
  - Technology (e.g. detection)
  - Policies
  - Treaties and partnerships
- How much should be spent to combat nuclear proliferation and nuclear terrorism?

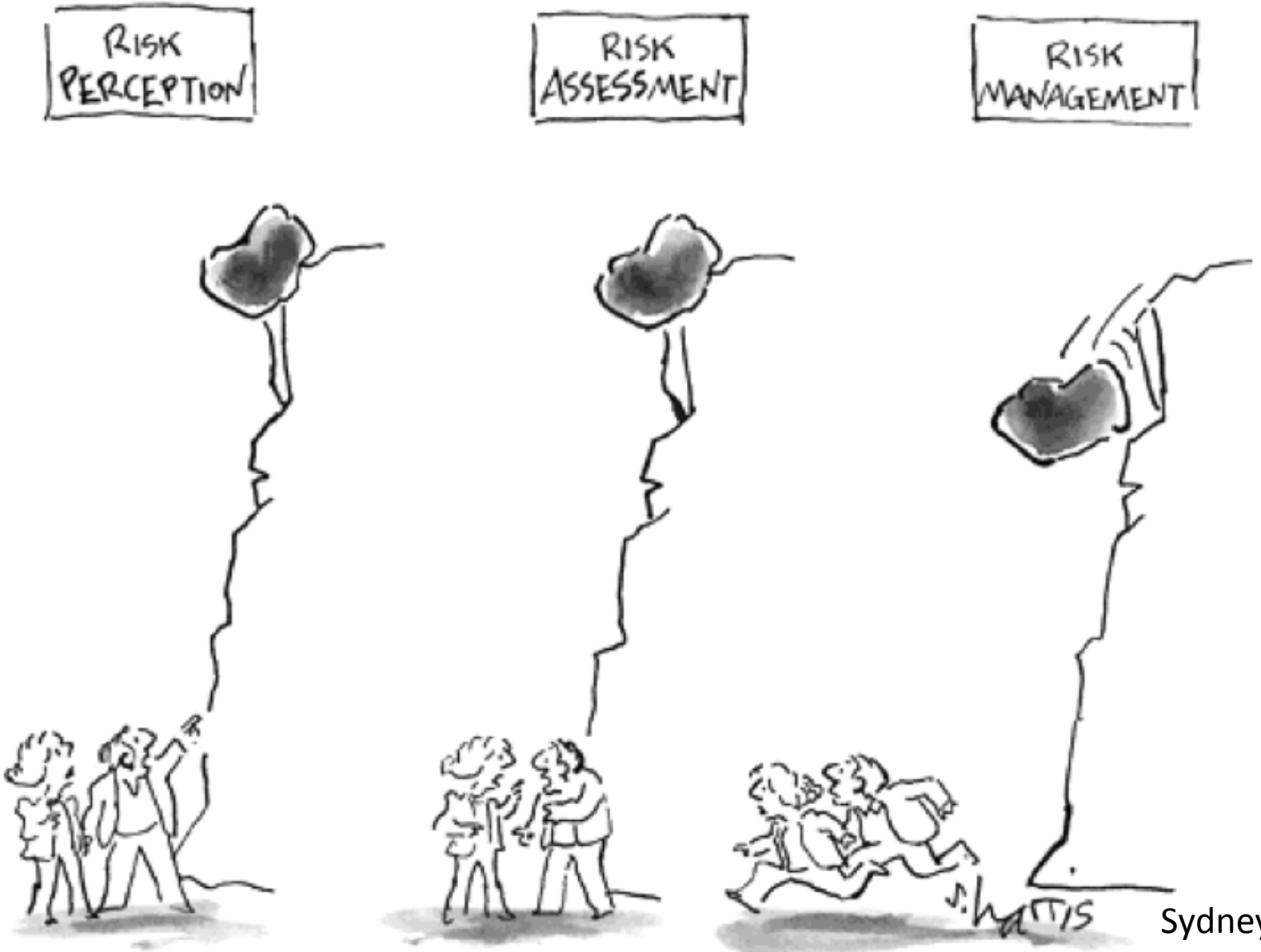
http://web.ornl.gov/sci/nsed/gnstd/

Early on, these questions tended to get answered in one of two ways.

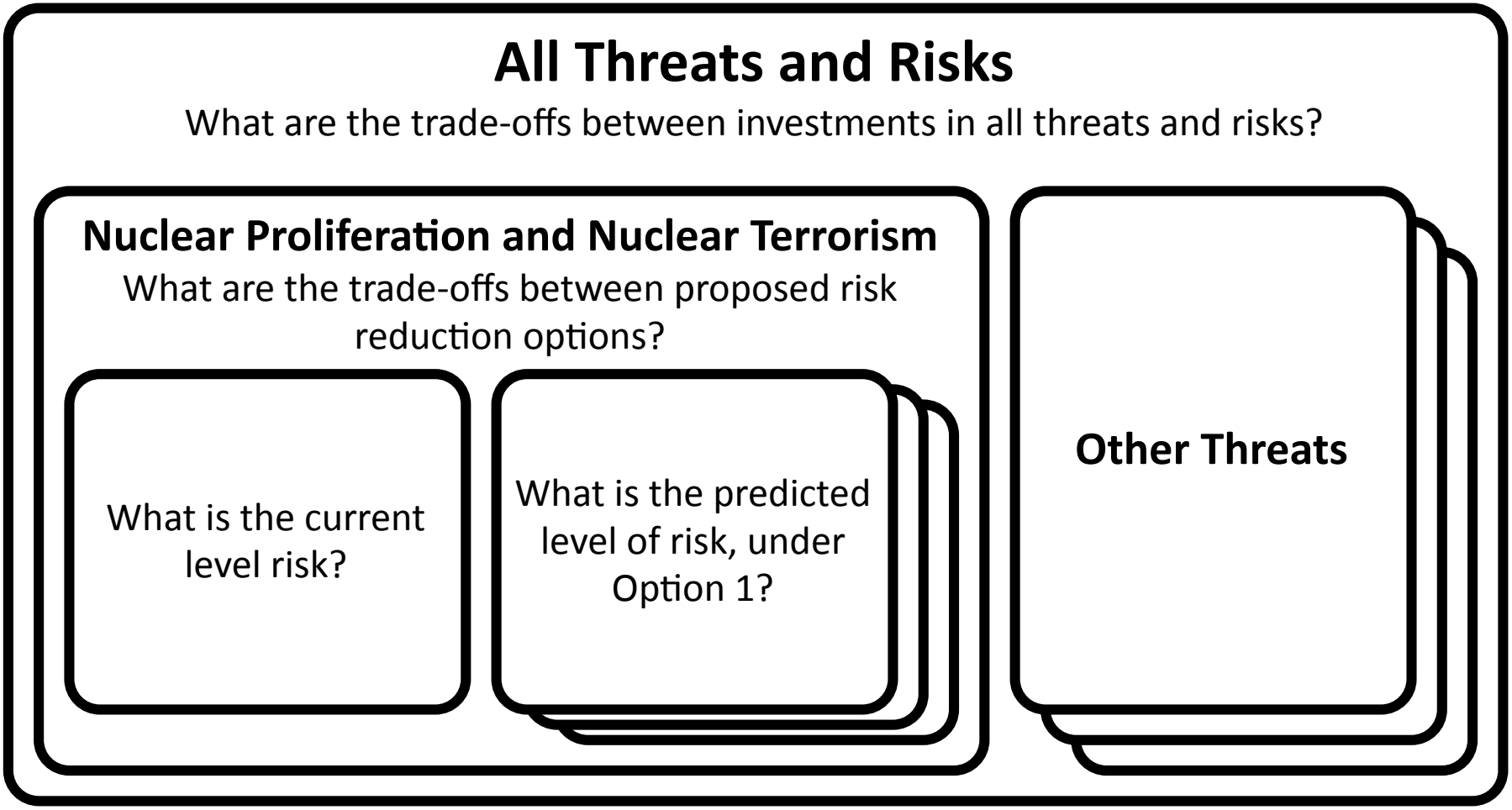
- Reactions to real world events
  - Posto attack or posto event environments tend to set priorities, free up resources, and provide focus
- Discipline focused narratives
  - Advocates have specific training that greatly influences how they view problems and solutions
  - Specific technical solutions to sub-problems are easier to analyze
    - Performance metrics
    - Alternatives

The resulting measures often have significant value, but there are benefits in being more systematic…

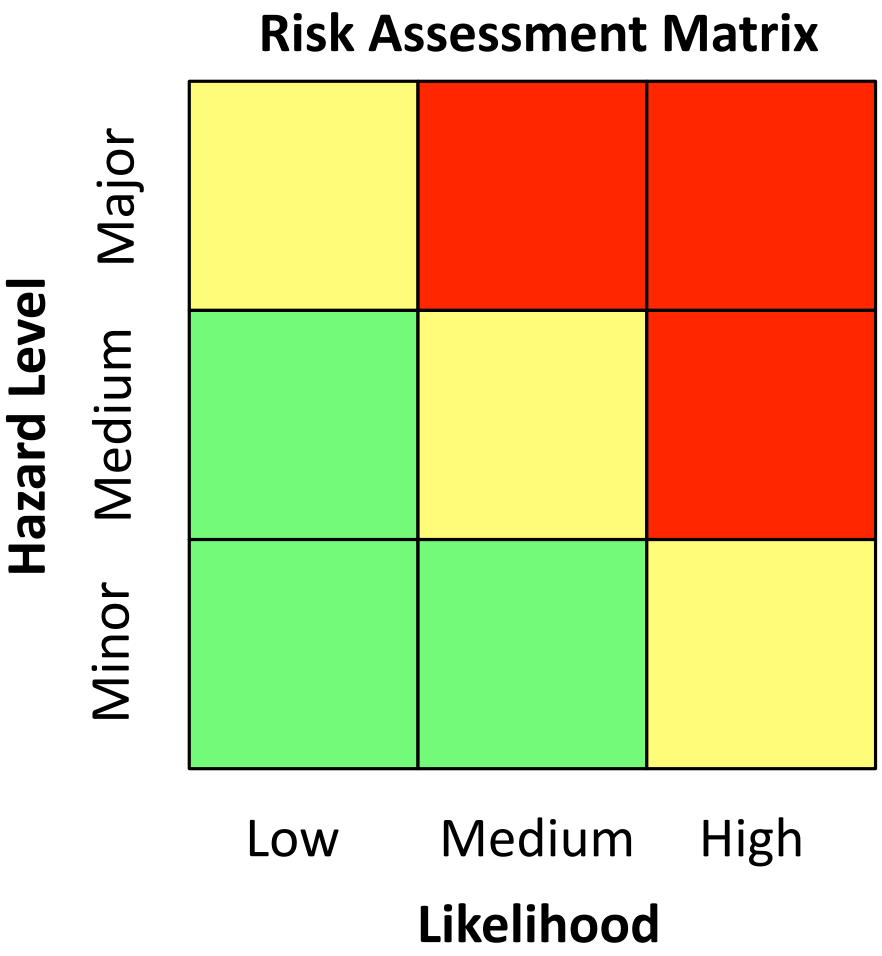
Risk analytic techniques offer a tempting framework for analysts.



Important questions to a risk analyst:



Risk matrices are a common, though ad hoc, analytic technique.



- Benefits
  - Motivates specific discussion of threat
  - Requires consensus among those involved
- Drawbacks
  - Difficult to repeat
  - Imprecise definitions
  - Inconsistent interpretations
  - Dependencies are not well captured

A More Precise Definition of Risk Analysis

Risk analysis is a scientific and systematic assessment of possible outcomes (usually hazards) their likelihoods.

- Level 0: Identification of Hazard
- Level 1: Worst Case Assessment
- Level 2: Plausible Upper Bound
- Level 3: Point Estimates and Average Cases
- ***Level 4: Probabilistic Risk Analysis***
- Level 5: Epistemic Uncertainty PRA

Paté-Cornell, *Uncertainties in Risk Analysis: Six Levels of Treatment*, Reliability Engineering & System Safety, Vol. 54, No. 2-3, 1996, pp. 95-111

A Brief History of Risk Analysis

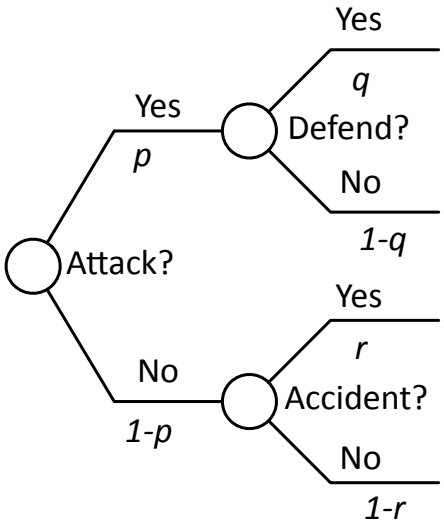
- 3200 BCE – The Asipu become the first "consulting firm" and use a systematic method, but no uncertainty
- 4th Century CE – Arnobius uses a systematic method, with uncertainty to argue why he wants to convert to Christianity, first example of probabilistic "dominance", but no probability
- 1657 – Pascal introduces probability theory
- 1693 – Halley performs a statistical analysis of births and deaths, refutes mystical explanations of mortality
- 1763 – Price posthumously publishes Bayes' theorem
- 1792 – LaPlace develops the first modern quantitative risk analysis, examines smallpox vaccinations

A Brief History of Risk Analysis

- 1898 – Bortkiewicz publishes analysis of Prussian horse kick accidents, along with an analysis of possible alternatives
- 1933 – Kolmogrov lays the axiomatic foundations of modern probability theory
- 1944 – von Neumann begins the modern field game theory
- 1946 – Konopinski, Teller, and Marvin use nuclear physics and qualitative uncertainty to examine catastrophic effects of thermonuclear devices
- 1964 – Howard and others found the field of Decision Analysis
- 1981 – Kaplan and Garrick define modern risk analysis, $R=f(T,V,C)$
- 1981 to Present – Expansive use of quantitative risk analysis to a broad array of engineered and natural systems…

There are many, well-developed, mathematical tools available.

Event Trees

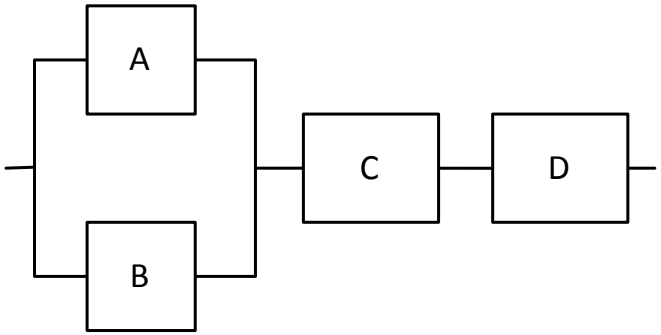


Game Theory

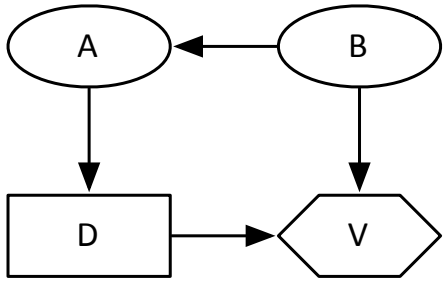
Player 1 \ Player 2	Confess	Refuse
Confess	1, 1	2, 0
Refuse	0, 2	3, 3

Optimization Theory

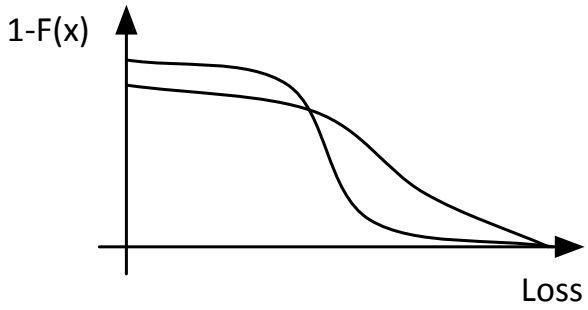
$$\begin{aligned} \min_x \quad & g(x_1, x_2, x_3) \\ \text{s.t.} \quad & x_1 + x_2 \leq B \\ & x_2 - 3x_3 \leq 10 \\ & x_1, x_2, x_3 \geq 0 \end{aligned}$$



Function Block Diagrams and Fault Logic



Decision Analysis



Probability Theory

Nuclear Nonproliferation Risk Analysis in the Academic Literature

- Much of the work on nonproliferation has been focused on treaty compliance and verification games, and incentives:
  - Dresher, *A sampling inspection problem in arms control agreements*, RAND, 1962
  - Weissenberger, *Treaty verification with an uncertain partner*, No. UCRL-JC-105885, CONF-9106112-1, Lawrence Livermore National Lab., CA (USA), 1991
  - Avenhaus, *Inspection games in arms control*, European Journal of Operational Research, 90.3 (1996), pp. 383-394
- More recent work has actually looked at assessing probabilities of nuclear proliferation under different policies
  - Caswell et al., *Analysis of national strategies to counter a country's nuclear weapons programs*, Decision Analysis, Vol. 8, No. 1, March 2011, pp. 30-45

Terrorism Risk Analysis in the Academic Literature

- Since, 2001, terrorism has been an increasing focus in the risk analysis literature.
- Some have been focused on methods
  - Paté-Cornell and Guikema, *Probabilistic modeling of terrorist threats: A systems analysis approach to setting countermeasures*, Military Oper. Res. Vol. 7, No. 4 (2002), pp. 5-24
  - Zhuang and Bier, *Balancing terrorism and natural disasters – Defensive strategy with endogenous attacker effort*, Operations Research, Vol. 55, No. 5 (2007), pp. 976-991
  - Ezell et al., *Probabilistic Risk Analysis and Terrorism Risk*, Risk Analysis, Vol. 30, No. 4 (2010), pp. 575-589
  - Rios Insua et al, *Adversarial Risk Analysis*, Journal of the American Statistical Association, Vol. 104, No. 486 (2009), pp. 841-854
  - Yang et al., *Improving resources allocation strategies against human adversaries in security games: An extended study*, Artificial Intelligence, Vol. 195, 2013, pp. 440-469
- Many have been focused on specific problems
  - von Winterfeldt and O'Sullivan, *Should we protect commercial airplanes against surface-to-air missile attacks by terrorists?*, Decision Analysis, Vol. 3, No. 2 (2006), pp. 63-75

Nuclear Terrorism Risk Analysis in the Academic Literature

- Early work focused on high level models
  - Bunn, *A mathematical model of the risk of nuclear terrorism*, Annals of the American Academy of Political and Social Science, Vol. 607, No. 1 (2006), pp. 103-120
- Later work examined specific applications
  - Bakir, *A Decision Tree Model for Evaluating Countermeasures to Secure Cargo at United States Southwestern Ports of Entry*, Vol. 5, No. 4 (2008), pp. 230-248
  - Merrick and McLay, *Is Screening Cargo Containers for Smuggled Nuclear Threats Worthwhile?*, Decision Analysis, Vol. 7, No. 2 (2010), pp. 155-171
  - Feng and Keller, *A multiple objective decision analysis for terrorism protection: Potassium-iodide distribution in nuclear incidents*, Decision Analysis, Vol 3., No 2 (2006), pp. 76-93
  - … and on, and on …

A quick review:

- Nuclear nonproliferation and terrorism are complex, unsolvable problems, that must be managed
- Risk analysis tools are sophisticated and well-developed, have been extensively explored for nuclear threats, and have been applied
  - Extensive academic research
  - Government (e.g. RNTRA)

So, why aren't risk analytic methods used more? Why isn't this a solved problem?

“Your technical analysis is very interesting.

However, we have decided to ignore it.”

Risk analytic methods in nuclear threat management face 4 critical challenges:

1. Lack of unanimity
   - Definition of Risk
   - Included Scenarios
   - Adversary models
   - Empirical data
2. Lack of high-level problem description
3. Lack of integrating methodology
4. Lack of persistent, singular effort

Challenge 1: Lack of Unanimity

A decomposition of a possible definition of risk:

Risk Definition:
- Metrics and Units
- Risk Preferences
- Distributions vs. Expected Values

$$R = \sum_{\forall A} P(A) \cdot P(S|A) \cdot C(A)$$

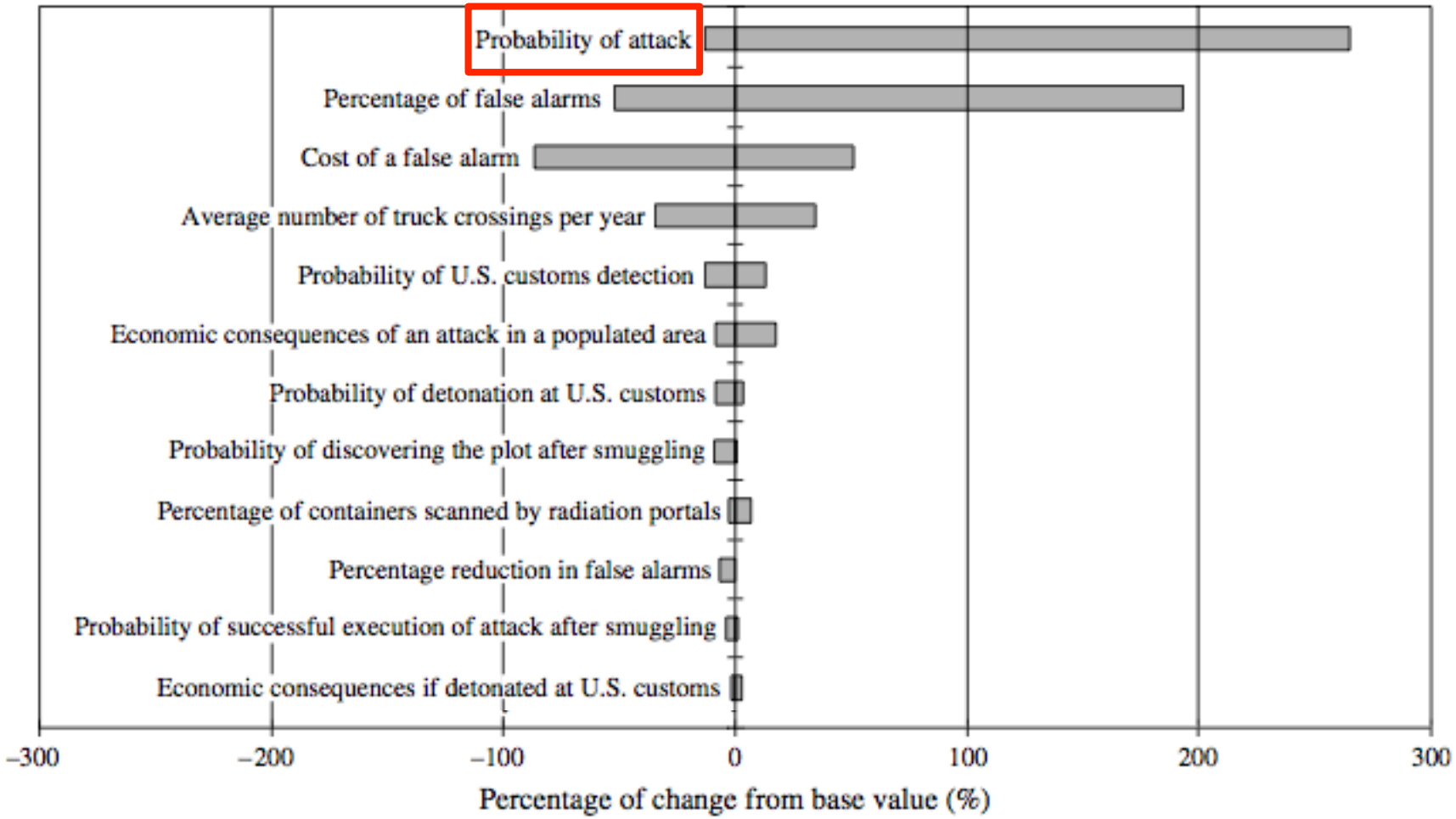
Attack Scenarios:
- Which are included?

Adversary Models:
- Probabilistic vs. Game Theory
- General vs. Specific
- Objectives and values
- Biases and information
- Reaction to countermeasures

Limited Empirical Data:
- Events are infrequent and unique
- Testing is resource intensive
- Subjective v. Frequentist Prob.

Adversary models are important!

Sensitivity of Equivalent Economic Cost to Significant Parameters



From Figure 4 in Bakir, 2008

Methods to model adversary choices has been a central area of debate.

- U.S. National Research Council 2008 report[1]
  - Probabilistic representations of adversaries is insufficient
  - Adversaries must be modeled as "intelligent" using decision methods to choose among alternatives and responsive to countermeasures
  - Attack probabilities are *outputs* of models, not *inputs*
- Other issues have been raised in the literature[2,3]
  - Different models of adversary objectives and decision rules have large effects on recommendations
  - Outguessing regress (i.e. common knowledge) is a cofounding problem for models
  - Implementation of recommendations can inform adversaries

[1]Committee on Methodological Improvements to the Department of Homeland Security's Biological Agent Risk-Analysis, *Department of Homeland Security Bioterrorism Risk Assessment: A Call for Change*, National research Council, 2008, available at: http://books.nap.edu/openbook.php?record_id=12206

[2]Brown et al., *How probabilistic risk assessment can mislead terrorism risk analysts*, Risk Analysis, Vol. 31, No. 2 (2011), pp. 196-204

[3]Merrick and Parnell, *A comparative analysis of PRA and intelligent adversary methods for counterterrorism risk management*, Risk Analysis, Vol. 31, No. 9 (2011), pp. 1488-1510

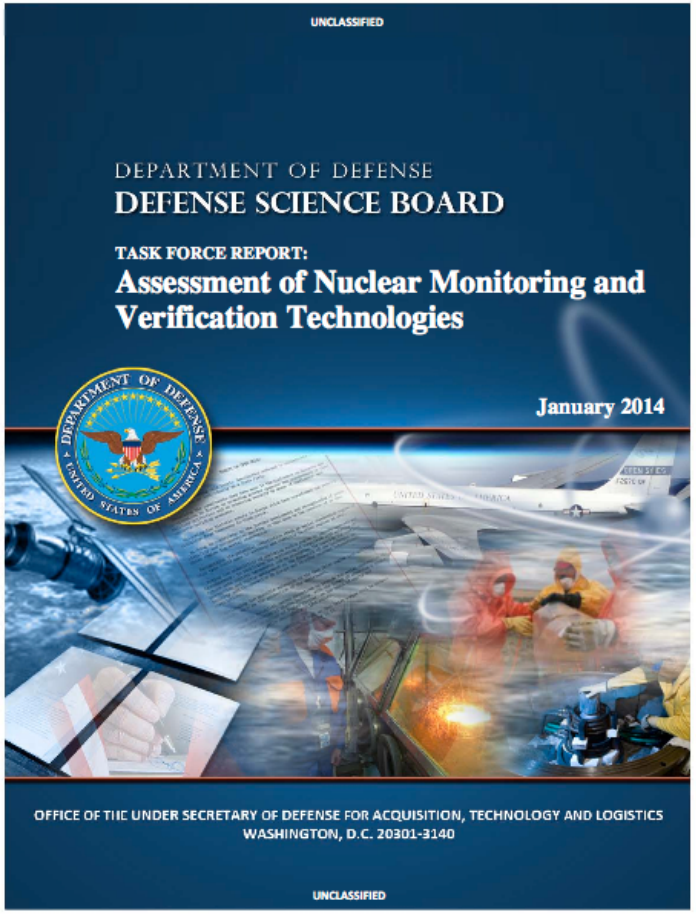
A lack of unanimity among analysts leads to a lack of credibility.

- Each of the choices an analyst must make is inherently a personal judgment
  - Implicitly limits the scope of the analysis and the applicability of the results
  - Policy makers and other analysts may not share the analysts view
  - Results and recommendations become fragile to "what-ifs"

- Current recommendations are towards plurality in models (e.g. Ezell et al., 2010, Lathrop et al., 2012)
  - The trade-off is now between judgment and complexity
  - How do you combine the results?

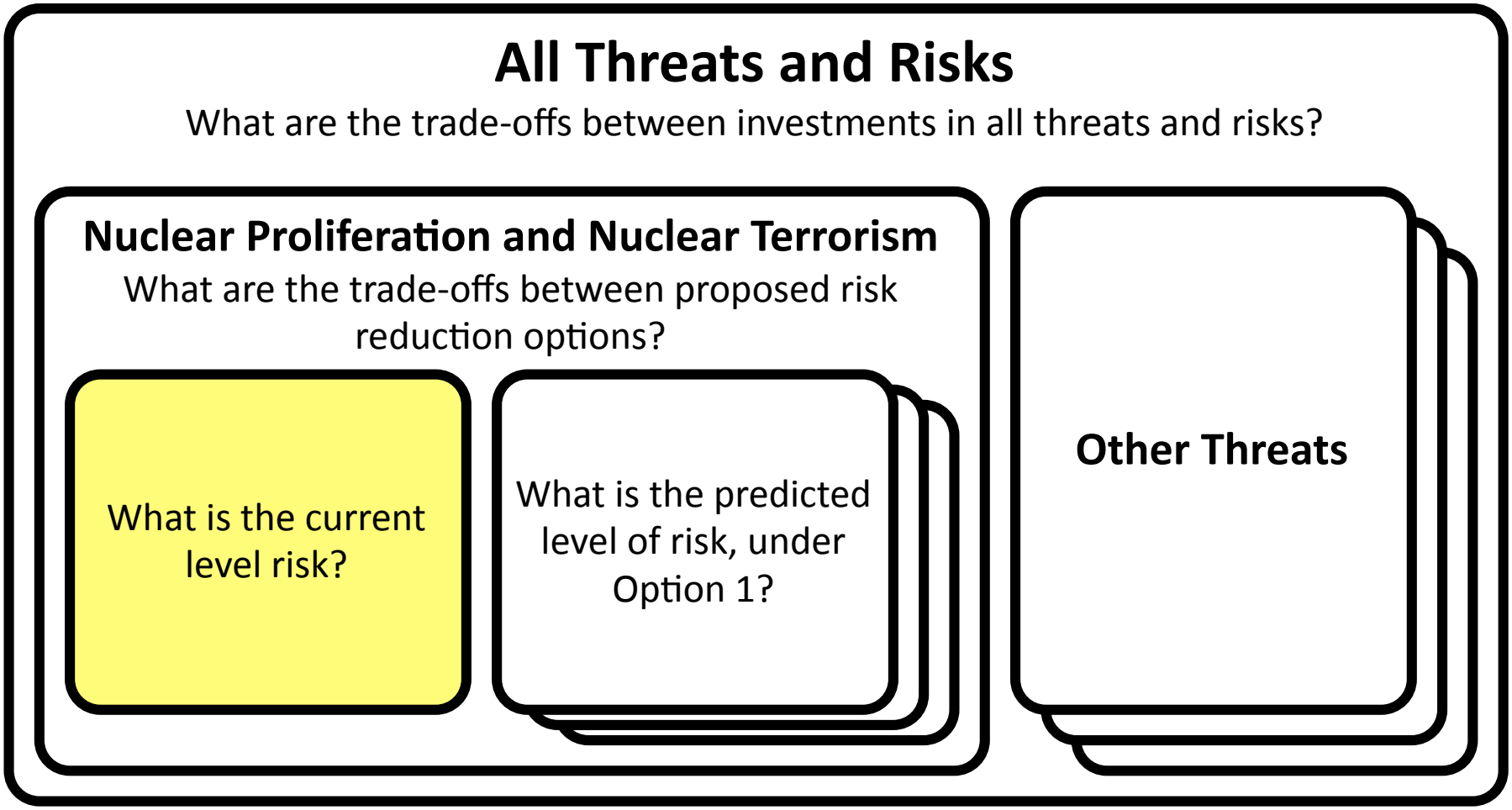
A recent Defense Science Board report discusses the next three challenges.

- Provides a future forecast of global nuclear issues to inform priorities
- Assesses current technologies and programs
- Provides recommendations for future investments and research
- *Specifically addresses problems of capability analysis, assessment, and integration*



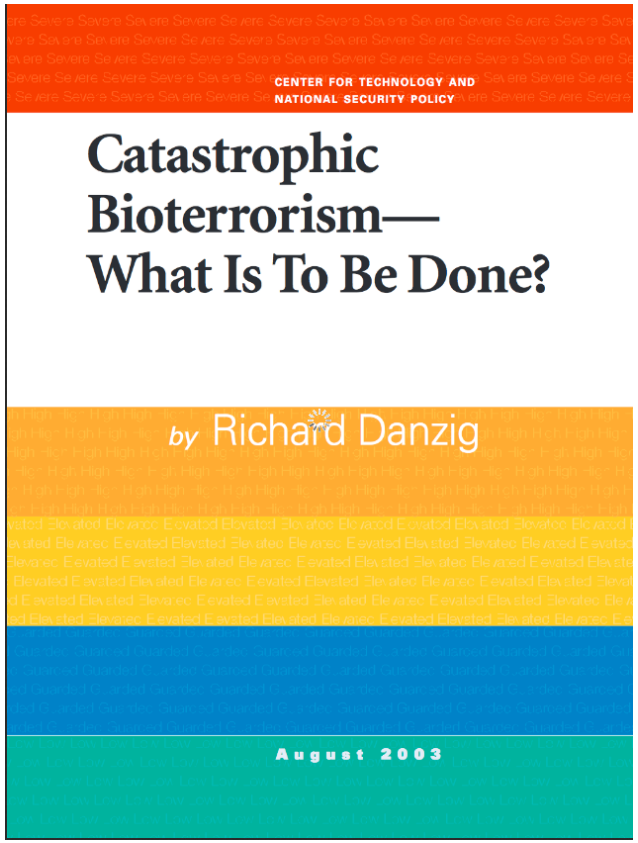
Defense Science Board, *Task Force Report: Assessment of Nuclear Monitoring and Verification Technologies*, Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics, January 2014, available at: http://www.acq.osd.mil/dsb/reports/NuclearMonitoringAndVerificationTechnologies.pdf

Challenge 2: Lack of High-Level Problem Description



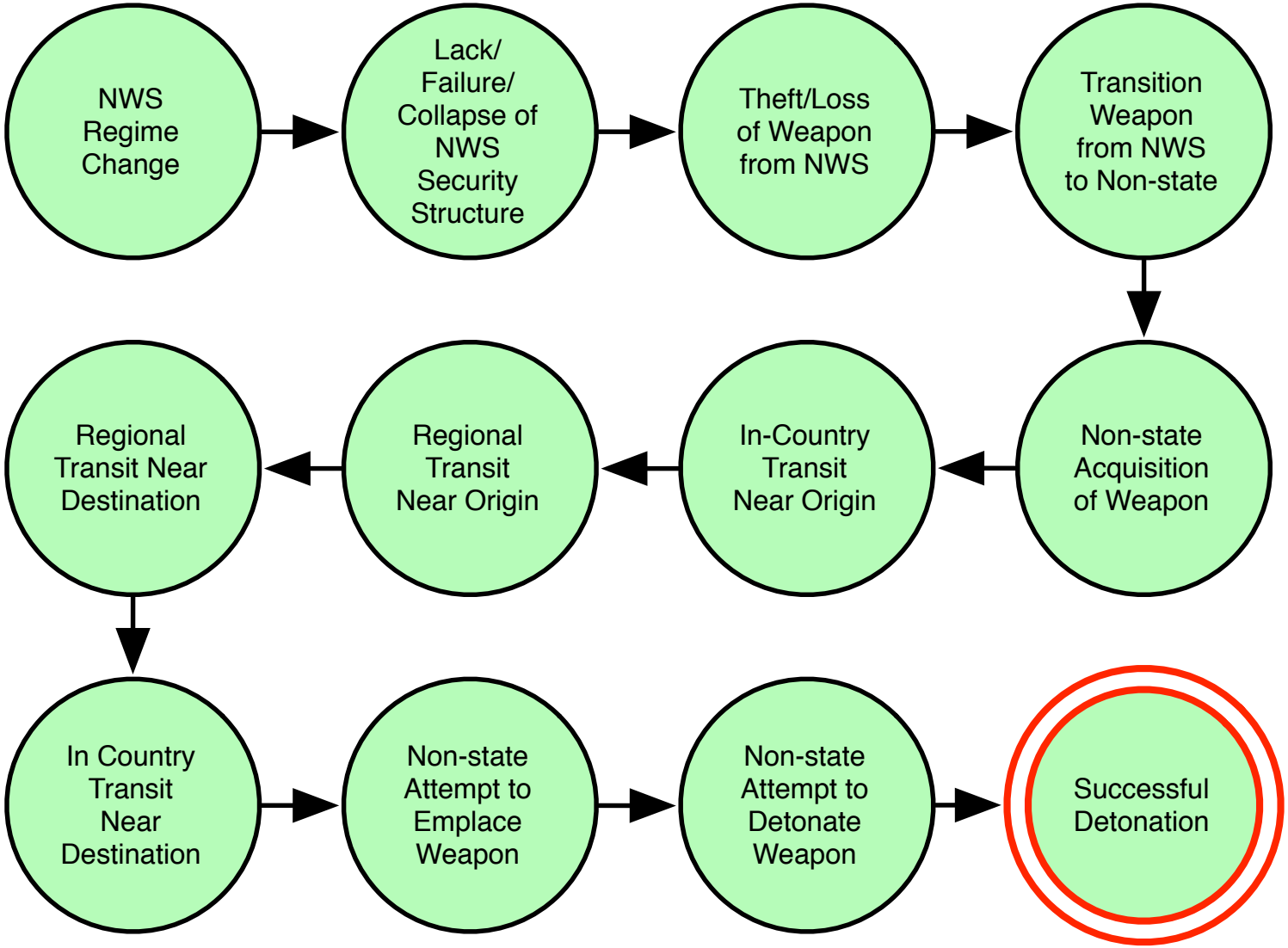
Scenario analyses are common approaches to complex problems.

- Danzig summarized the issues for multi-agency, multi-state response to global threats
  - Individual efforts tend to be unrelated to any overarching strategy
  - High-level metrics are difficult to formulate
  - Capabilities and countermeasures tend not to be viewed as alternatives or complements, but as competing or independent programs
- Proposed a set of five planning scenarios to help organize efforts
- Small sets of planning scenarios are helpful, but can still be limiting
  - Provides problem description that does not include proposed solutions
  - Becomes foundation for high-level evaluation metrics
  - Unclear how to trade-off between scenarios, and how they might depend on each each other

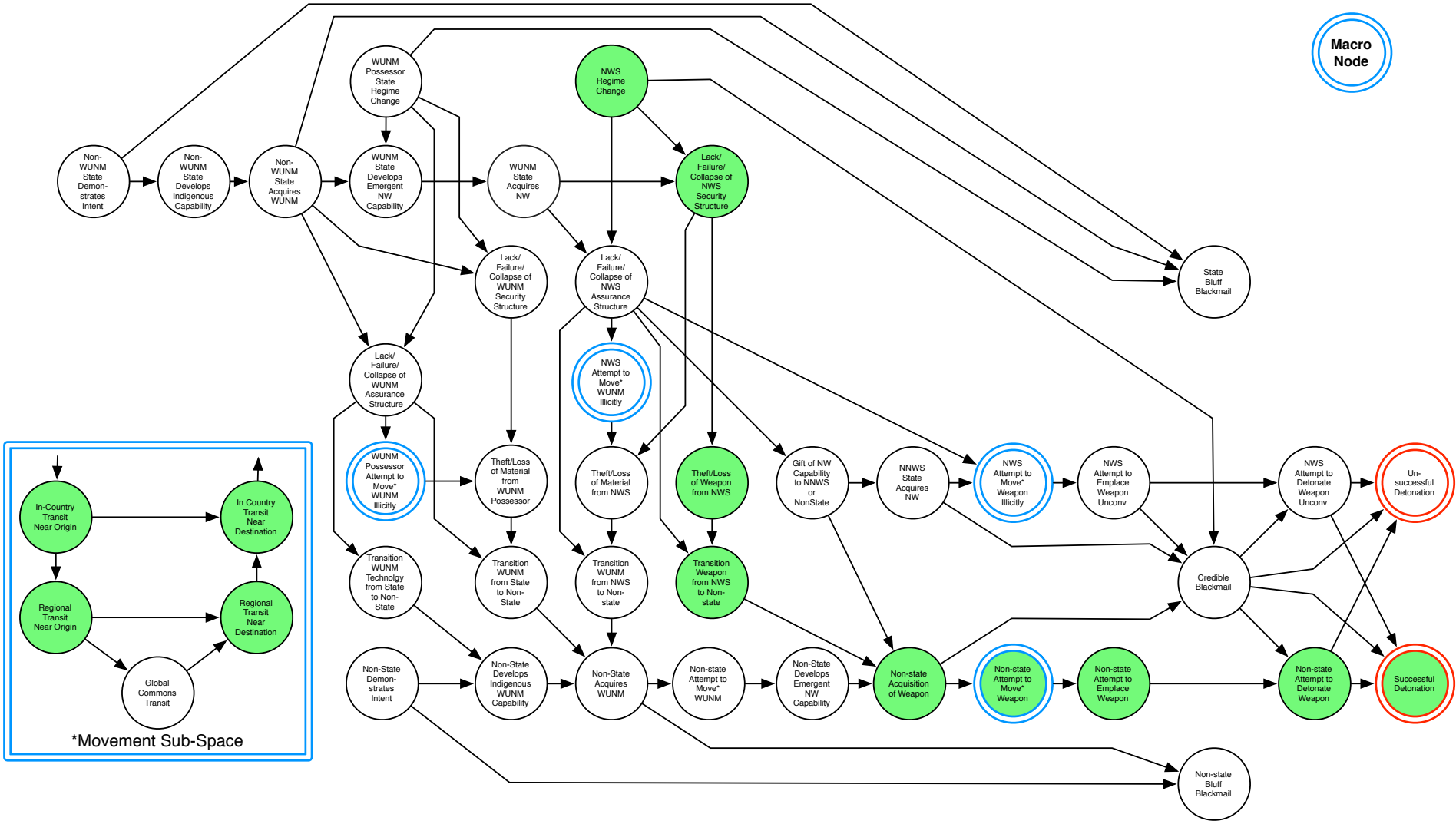


Danzig, *Catastrophic Bioterrorism – What is to be done?*, Center for Technology and National Security Policy, August 2003

Scenarios can be broken down into evolutions of discrete steps.



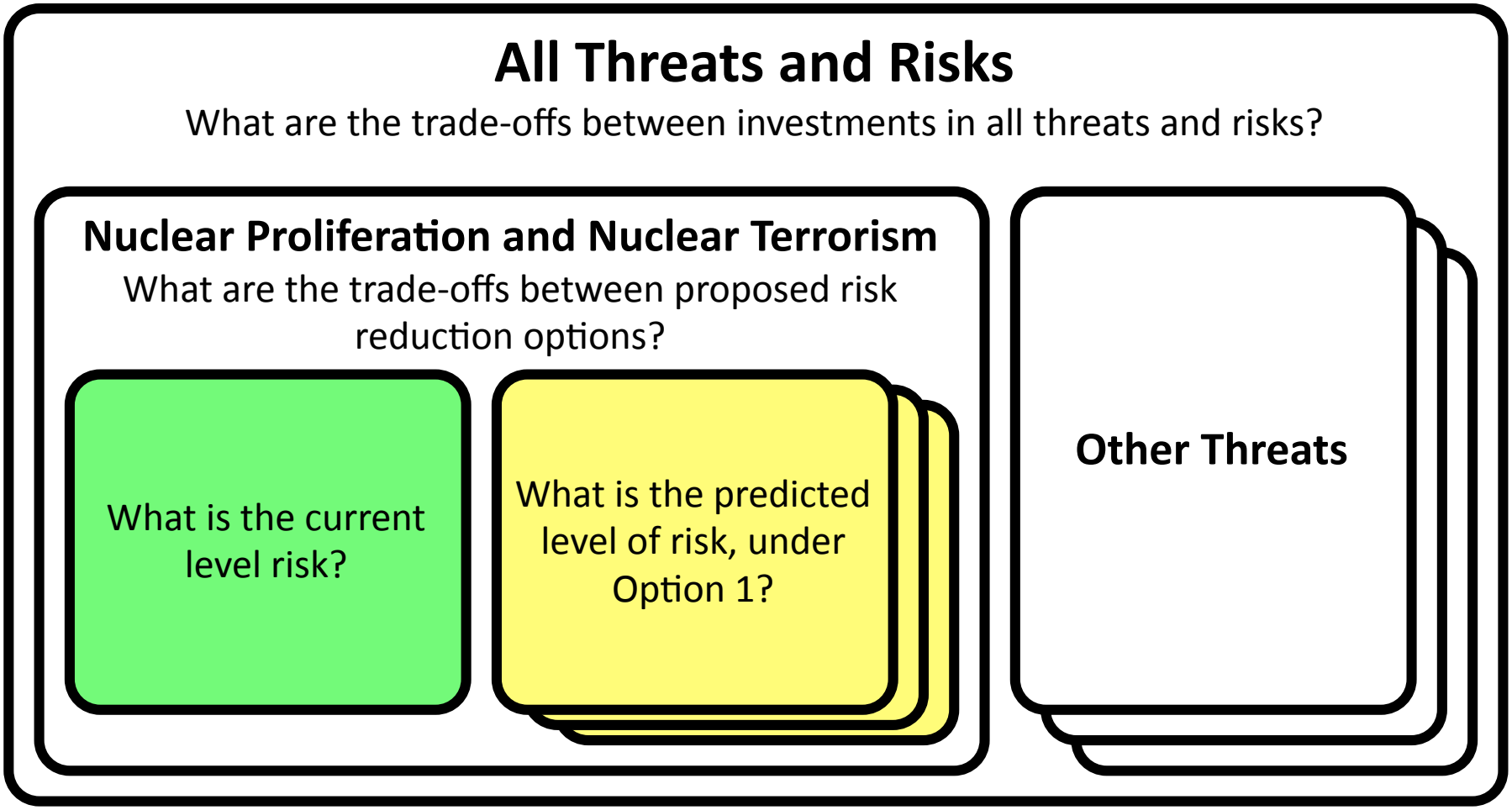
Families of scenarios can be linked together to describe a broad threat.



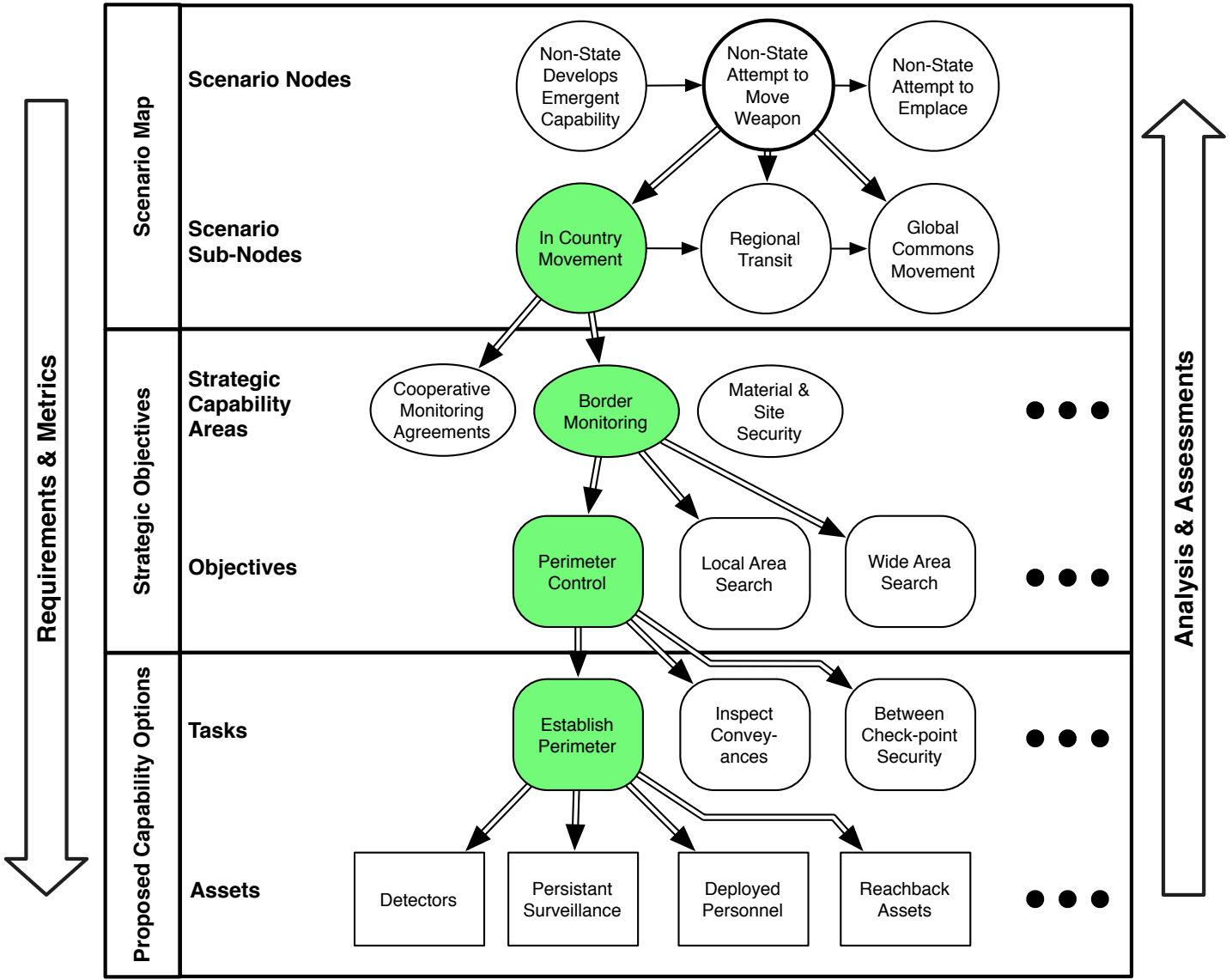
A scenario map as a common, high-level problem definition has benefits.

- Brings structure to an already vigorous debate
- Promotes development and consideration end-to-end metrics over subsystem performance
- Identifies relationships between proposed solution strategies
- Scenario maps allow for the problem to be deconstructed in a different way than traditional scenario-based analyses

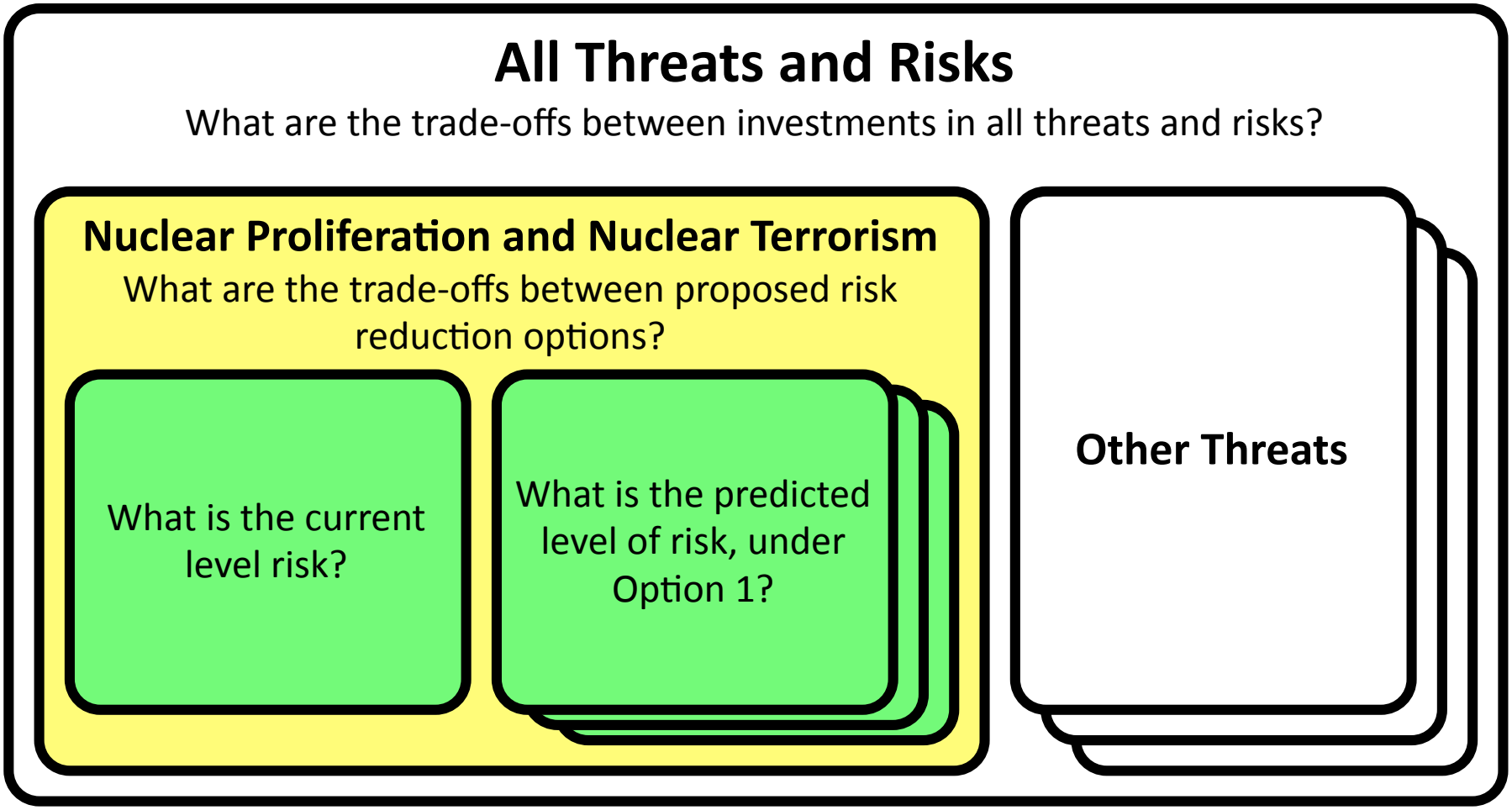
Challenge 3: Lack of Integrating Methodology



Scenario map nodes must be deconstructed to investment alternatives.



Challenge 4: Lack of Persistent, Singular Effort



Challenge 4:

- There are many distinct efforts looking at various aspects of nonproliferation and nuclear terrorism risk.
  - Academia
  - Institutions
  - Governments
  - Super-national entities

- The methods used to set priorities for countermeasure and capability development in nuclear nonproliferation and nuclear counter terrorism is, itself, a countermeasure
  - Most efforts focus on singular scenarios, or lower levels
  - Concerted effort to develop a higher-level cohesive approach are critical to making progress

An overarching, and persistent analytical capability should be established with both dedicated focus and authority.

Collaboration on nuclear nonproliferation and countering nuclear terrorism

- There is a precedent at many levels:
  - Treaties and agreements
  - Material and site security
  - Nuclear Security Summits
  - Global Initiative to Combat Nuclear Terrorism (GICNT)
    - Detection architectures
    - Forensics
  - Operational cooperation
- Most of these focus on developing
  - Collaborative authorities and norms
  - Guidelines for implementation
  - Countermeasures (e.g. detection)

Collaboration on analytical challenges should be an area of development.

- Partner nations should work together to adopt:
  - A common over-arching framework
  - Common end-to-end metrics
  - Co-developed methods for risk analysis and assessment
- Joint leadership sets a powerful precedent and can align broad, and disparate efforts
- Shared assessments and data can strengthen analytical results
- Joint analytical plans from partner governments, and adoption of results in setting national priorities can focus debates and foster increased collaboration capability development

The more we share in how we think about the problem, the better we can jointly address vulnerabilities and threats.